Remarks:

Reconsideration of the above referenced application in view of the enclosed amendment and remarks is requested. Claims 1, 7, 8, 11, 15, 17, 23, 24 and 27 are amended. Claims 2, 12 and 18 are canceled. Claims 1, 3-11, 13-17, and 19-32 remain in the application.

ARGUMENT

35 U.S.C. § 112 Rejections:

Claims 8-16, 24-26 and 32 are rejected under 35 U.S.C. §112 first paragraph, as failing to comply with the description requirement. This rejection is respectfully traversed and Claims 8-16, 24-26 and 32 and their progeny are believed allowable based on the above amendments and the following discussion.

The Examiner asserts that the specification does not teach "when a message from an authorized party is not received as a BIOS; booting the system without enabling the optional features." One of ordinary skill in the art will understand the difference between default features and optional features. If there are no optional features selected, then the system will boot in a default mode. The alternative is that the system will not boot at all, as shown by the cited prior art (Tello), but not taught by Applicant. Applicant's description in the specification does not teach or describe that the claimed invention fails to boot when no options are selected. The feature of booting without enabling optional features is inherent in the invention and will be understood by one of ordinary skill in the art. For instance, in the specification on pages 4 and 5, it is said "The capability of enabling optional system features is preferably secure, because the OEM may not want the system features to be enabled without authorization." As will be understood by one of ordinary skill in the art, if an optional feature is not authorized, the system will boot without optional features, e.g., in a default mode. Moreover, the Applicant describes on page 8, lines 10-13 of the specification that "If failure occurs (blocks 411, 412, and 413) during the decryption, authentication, or verification, process 40 is aborted, and the message is discarded (block 49)." As described on page 8, lines 1-2, "process 40 is shown for enabling

optional system features of system resources 25." At no time does the Application teach, suggest or imply that the system does not boot. It is only described that enabling the optional system features process is aborted. It will be apparent to one of ordinary skill in the art that the system will continue to boot without enabling the optional feature because the message failed to be authenticated. At no time is it described that the boot process, as a whole, is aborted. Moreover, the specification describes, at least in conjunction with Fig. 2, that a message may be received while the system is already booted and that a reboot may be required. It will be obvious that if an authorization message is to be received while the system is running that it had to boot in some default state prior to receiving the message.

It will be understood that the optional features described in the specification are to allow the OEM or vendor to control the processing power, available memory, or other processing power features of a system. As described in the Specification, controlling the optional features enables the OEM to manufacture fewer SKUs of systems, while maintaining various price points or operational feature for various customers. A minimum system may be purchased without enabling the optional system resources. If no optional features are to be authorized, the system will still boot in a default state. This is inherent by virtue of the fact that the system resources having controllable optional features are described as features such as storage capacity, processor redundancy, processor speed, memory, input/output devices, processors, redundant power supplies, Peripheral Component Interconnect (PCI) bus, and other elements of the system contributable to processing power. It will be apparent to those skilled in the art that the optional features enable increased processing power or storage capacity. The term "optional" is commonly understood and defined, for instance, at URL *www*answers*com/topic/optional*, as

"*Left to choice; **not compulsory** or automatic.*" [emphasis added]

It will be obvious to those skilled in the art that by using the term "optional" throughout the description and as recited in the claims that these features are not compulsory to operate the system. As such, it will also be obvious to those skilled in the art that if optional features are not authorized (i.e., no validated message received) that the system will boot without the optional features. To assume any other meaning of the term "optional" in context of the disclosure and recited claims would be inconsistent with the commonly understood meaning of the term

"optional." It should be noted that periods are replaced with asterisks in URLs to avoid inadvertent hyperlinks.

Specifically regarding the additional rejection for Claims 24-26, it would appear that the Examiner has misunderstood the basic premise of Applicant's invention regarding the meaning of optional features. For instance, the citation of Tello as prior art is not analogous. Tello is a system for authenticating a user based on validating a smart card with a system to authorize use. The enabling of system resources based on the identity of the user is secondary, and not performed in the manner of Applicant's recited claims. McKnight et al. is also misapplied and that system is directed toward use of a network of hosts for providing services and does not relate to providing optional features to increase platform processing power or storage capacity. It will be apparent to those skilled in the art that a system may be booted with or without the optional features, by nature of the meaning of "optional." The Examiner asserts that the system as described by Applicant "should always have optional features." To avoid the Examiner's confusion, Applicant amends Claim 24 to recite *booting the system without enabling optional features of the system*. The term "enabling" is added to avoid the perception that the system doesn't have optional features, but that it is merely booted without enabling the optional features, i.e., increased processing power or storage capacity. Therefore, Claims 8-16, 24-26 and 32 are believed allowable.

Claim 32 is rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Specifically, the Examiner asserts that "wherein the system comprises a platform to authenticate the secure message by the BIOS without requiring additional processor or hardware." This rejection is respectfully traversed and Claim 32 is believed allowable based on the following discussion.

Page 6, lines 19-23 of the Specification describe that:

> "**The BIOS** 22 at the final destination of the feature packet (i.e., system 10) **can perform complete authentication and validation of the feature packet's content** regardless of the transmission medium and/or number of time the feature packet is transferred." [emphasis added]

It is described that the platform BIOS can perform the complete authentication and validation of the secure message, regardless of how the packet/message is transferred. It will be

apparent to one of skill in the art that when the BIOS receives a secure message to control optional features that it requires no other processor or hardware to complete the authentication and verification. The specification clearly describes that the complete authentication and verification is performed by the BIOS. It will be understood by those of skill in the art that the BIOS is part of the system as exists in the art and if the BIOS performs something completely, then no other additional hardware or processor is necessary to perform the invention. This is contrary to the cited references, for instance, Tello (Fig. 1), which requires a security engine microprocessor 125, a smart card reader 133, a smart card 135, a smart card (not shown), etc. It will be obvious that Applicant's claimed invention provides an advantage over the cited prior art in that it does not require additional hardware to operate.

Claim 32 is rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to point out and distinctly claim the subject matter of the invention. This rejection is respectfully traversed and Claim 32 is believed allowable based on the foregoing and following discussion.

Applicant amends Claim 32 to recite that the system comprises *a platform to authenticate the secure message by the BIOS without requiring a processor or hardware in addition to hardware used in the system to execute the BIOS, in order to perform the authentication*. This amendment is merely grammatical to ensure that it is understood that the system hardware and firmware needs no supplement in order to authenticate the message. The BIOS and system firmware and hardware perform the message authentication without requiring an additional processor or additional firmware. This is in contrast to the cited references, as discussed above. Support for this limitation is also discussed above. Thus, Claim 32 is believed allowable.

35 U.S.C. § 102 Rejections:

Claims 1, 8, 17, 24 and 27 are rejected under 35 U.S.C. § 102(c) as being anticipated by U.S. Pat. No. 6,463,537 to Tello (hereinafter, "Tello"). This rejection is respectfully traversed and Claims 1, 8, 17, 24, 27 and their progeny are believed allowable based on the above amendments and the foregoing and following discussion.

The Examiner cites Tello, Col. 4, lines 11-37 to show authenticating the message. This rejection is improper, based on the cited reference, and should be withdrawn. At Col. 4, lines 11-37, Tello teaches that each peripheral device has a digital signature. Thus, activating approved peripherals requires the vendor or manufacturer to digitally sign the peripherals. This is contrary to Applicant's claimed invention, as amended, which requires, for instance, in Claims 1, 17 and 24, that *authenticating that the message has been sent by the authorized party using a digital signature in the message and a public key stored in non-volatile storage communicatively coupled to the BIOS* . At the cited reference, Tello does not teach that the public key of the digital signature is in storage accessible to the BIOS.

The Examiner also cites Col. 4, lines 11-37 or Tello to show that when the message fails authenticating, then discarding the message. This rejection is improper as Tello, col. 4, lines 11-37 do not explicitly teach or suggest discarding the message. At the cited reference, Tello merely teaches that each peripheral device has a digital signature to determine whether it is an approved device. Further, this is not an analogous art in that Tello describes authorizing peripheral devices and Applicant recites enabling optional features of system resources in the system. It will be apparent to one of skill in the art that peripheral devices are not system resources, as by definition, as peripheral, they are external to the recited system.

In addition, Claims 1, 8, 17, 24, and 27 have been amended to more clearly recite features of the verification aspect of Applicant's invention. Claims 1, 8, 17, 24 and 27 all require that verification that the system is the intended recipient of the message uses a globally unique identifier (GUID) of the system. As described and claimed, Applicant's invention requires both an authentication that the secure message is from an authorized party and that the recipient is the intended, verified recipient. This feature is not taught or suggested by Tello. Further, Claims 1 and 17 require *the GUID is stored in the non-volatile storage communicatively coupled to the*

BIOS. This is not taught or suggested by the cited prior art. Claims 8 and 24 require that the GUID is an *identifier of the system*. Claim 27 requires that the verification uses a GUID to *uniquely identify the system*. A GUID is commonly understood by those of skill in the art to be a unique identifier, usually 128-bits. None of the cited prior art teach or suggest that the system is to be uniquely identified in this manner. Therefore, the Examiner fails to present a *prima facie* case of anticipation or obviousness.

The Examiner cites McKnight et al., as showing that the authorizing party consists of a manufacturer, an original equipment manufacturer, and a lessor, as discussed with previously presented Claims 2, 11-12, 18 and 32. However, McKnight et al. is improperly combined with Tello, at least because it is not directed to analogous art, and as such, there can be found no motivation to combine Tello with McKnight et al. McKnight et al. teach a system for providing distributed computing services. McKnight et al. do not teach or suggest enabling optional features of a system resource, and thus is not related to the teaching of Tello at al. McKnight et al. teach a system for leasing services from a host on a distributed network of systems. There is no discussion of leasing or purchasing authorized features (system resources) within a single host or platform by an OEM or vendor. There is also no suggestion that this scheme would operate on such a system.

The Examiner also asserts that Tello teach verifying an identifier in the message against a unique system identifier (Col. 5, lines 15-48 and Col. 9, lines 26-30). Tello teaches that a complementary hash code is used to match a smart card with a system. This does not amount to a *globally unique identifier* for the system, as described and claimed by Applicant. Tello teaches that a digital signature is used (Col. 5, lines 21-24) is used to authenticate the user. This is contrary to Applicant's invention. Globally unique identifiers (GUIDs) are well defined in the art. A GUID is typically a unique 128-bit identifier which *uniquely* identifies something, in this case, the system. Applicant's claimed invention uses a digital signature to authenticate the sender of the message, but uses the GUID to verify that the platform in an intended recipient. Thus, there is a 2-step authentication and verification process which is not taught or suggested by the cited references. As understood by those of skill in the art, the digital signature uses a public/private key encoding/decoding, and the GUID verification requires a comparison or

regeneration of the actual GUID. Thus, Claims 1, 8, 17, 24, and 27 and their progeny are believed allowable.

Claims 1, 5, 8, 17, 21, 24-25 and 27 are rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Pat. No. 5,844,986 to Davis (hereinafter, "Davis"). This rejection is respectfully traversed and Claims 1, 5, 8, 17, 21, 24-25 and 27 and their progeny are believed allowable based on the above amendments and the foregoing and following discussion.

The Examiner asserts that Davis teaches authenticating the message at Col. 3, line 38 to Col. 4, line 18). However, Claims 1, 8, 17, 24 and 27 have been amended to recite *authenticating that the message has been sent by the authorized party using a digital signature in the message and a public key stored in non-volatile storage communicatively coupled to the BIOS* (Claims 1, 17, 24) and/or *verifying an identifier in the message against a globally unique system identifier (GUID) of the system* (Claims 8, 24, 27).

Davis merely suggests that authentication may use public/private key cryptography in a coprocessor. Davis does not teach or suggest that the public key is stored on non-volatile storage communicatively coupled to the BIOS. Further, Davis does not teach or suggest that the recipient is verified using a globally unique identifier (GUID). Moreover, Davis does not teach or suggest enabling an optional feature of a system resource. Davis merely teaches a method to upgrade a BIOS.

Regarding Claims 5, 21 and 25, the Examiner asserts that Davis teach *splicing the content of the message into an execution path of the BIOS, wherein the splicing comprises at least one of modifying the BIOS or erasing a portion of the BIOS, in response to the message.* However, Davis teaches only the replacement of the BIOS (see Col. 4, lines 14-18). An entirely new, replacement BIOS, is made operational and the entire previous BIOS is erased. This is contrary to well understood terms "splicing" and "portion." Applicant's claimed invention requires a *splicing* of the current BIOS. It will be well understood that *splicing* does not replace an entire BIOS and that a *portion* of the BIOS does not mean replacing the entire BIOS. Therefore, the Examiner has failed to provide a *prima facie* case of anticipation. Thus, Claims 1, 5, 8, 17, 21, 24-25 and 27 and their progeny are believed allowable.

35 U.S.C. § 103 Rejections:

Claims 1-4, 8-14, 17-20, 24, 27-28 and 32 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Tello in view of U.S. Publication 2002/0165819 to McKnight et al. (hereinafter, "McKnight et al."). This rejection is respectfully traversed and Claims 1-4, 8-14, 17-20, 24, 27-28 and 32 are believed allowable based in the foregoing and following discussion.

As discussed above with respect to amended Claims 1, 8, 17, 24 and 27, there is no motivation to combine the teachings of McKnight et al. with Tello. The Examiner asserts that it "would have been obvious to one of ordinary skill in the art at the time of the invention to combine the ideas of McKnight et al, with those of Tello and allow a lessor to configure a system in accordance with the teachings of Tello because doing so provides a convenient and secure way to enable certain resources." This argument begs the question. It is improper for the Examiner to fabricate a motivation or suggestion that is not made within the cited references. There is no motivation in Tello that would suggest that a method to lease networked services would be applicable to a system to enable optional features of system resources. Further, there is no suggestion in McKnight et al. that a system for leasing networked services could be expanded to include optional features of the system itself. The Examiner has improperly looked for an advantage of various unrelated features of the prior art and fabricated a convenient reason to combine them.

Applicant wishes to remind the Office of the bedrock legal principles for rejecting a claim under 35 U.S.C. § 103. Specifically, in In re Rouffet, 47 U.S.P.Q.2d 1453 (Fed. Cir. 1998) the Federal Circuit explained:

> To reject claims in an application under section 103, an examiner must show an unrebutted prima facie case of obviousness. In the absence of a proper prima facie case of obviousness, an applicant who complies with the other statutory requirements is entitled to a patent.

Id. at 1455 (citations omitted and emphasis added).

In the Rouffet case, the Examiner had rejected the pending claims on a combination of references. The Board sustained the Examiner. However, the Federal Circuit reversed the Board's decision and ruled that the Examiner's rejections were legally impermissible because

they failed to demonstrate a suggestion for combining the references in the manner proposed by the Examiner. As explained by the Federal Circuit:

> As this court has stated, "virtually all [inventions] are combinations of old elements." Therefore, an examiner may often find every element of a claimed invention in the prior art. If identification of each claimed element in the prior art were sufficient to negate patentability, very few patents would ever issue. Furthermore, rejecting patents solely by finding prior art corollaries for the claimed elements would permit an examiner to use the claimed invention itself as a blueprint for piecing together elements in the prior art to defeat the patentability of the claimed invention. Such an approach would be "an illogical and inappropriate process by which to determine patentability." To prevent the use of hindsight based on the invention to defeat patentability of the invention, this court requires the examiner to show a motivation to combine the references that create the case of obviousness.

Id. at 1457-58 (citations omitted and emphasis added). These principles have not been followed in rejecting Claims 1-4, 8-14, 17-20, 24, 27-28 and 32. Merely stating an advantage or possible advantage of combining references, as was done to reject Claims 1-4, 8-14, 17-20, 24, 27-28 and 32, is not the same as "show[ing] a motivation to combine the references."

On the contrary, in order to establish a *prima facie* case of obviousness, there must be actual evidence of a suggestion to modify a prior art reference or to combine two prior art references, and the suggestion to combine or modify the prior art must be clear and particular. In re Dembiczak, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). In order to establish a *prima facie* case of unpatentability, particular factual findings demonstrating the suggestion to combine must be made. See, for example, Ecolochem Inc. v. Southern California Edison, 56 U.S.P.Q.2d 1065, 1072-73 (Fed. Cir. 2000) and In re Dembiczak, 50 U.S.P.Q.2d 1614, 1617-1618 (Fed. Cir. 1999). Indeed, the law is quite clear that an obviousness rejection must be based on facts, not conjecture.

> The Supreme Court... foreclosed the use of substitutes for facts in determining obviousness under section 103. The legal conclusion of obviousness *must be supported by facts*. Where the legal conclusion is not supported by facts it cannot stand.

In re Warner, 379 F.2d 1011, 1017 (C.C.P.A. 1967). This longstanding principle has been followed to date. For example, in the unpublished Board decision, Ex parte Megens, App. No. 1999-0277 (B.P.A.I. Oct. 29, 1999), the Board stated:

> Rejections based on 35 U.S.C. § 103 must rest on a factual basis. In re Warner, 379 F.2d 1011, 1017, 154 USPQ 173, 177-78 (CCPA 1967). In making such a rejection, an examiner has the initial duty of supplying the requisite factual basis and may not, because of doubts that the invention is patentable, resort to speculation, unfounded assumptions or hindsight reconstruction to supply deficiencies in the factual basis. Id.
>
> The examiner's conclusion that it would have been obvious to incline Phillips' loading dock floor 65 rests on the completely unfounded assumption that it would be desirable to drain liquid from the floor. The Phillips reference, however, is devoid of any indication that liquid might accumulate on the floor or that such accumulation would pose a problem even if it did occur. It is therefore apparent that the examiner has resorted to improper speculation and hindsight reconstruction to overcome the admitted deficiency of Phillips vis-à-vis the subject matter recited in claim 1.

(Megens at Pages 4-5)(emphasis added).

Further, neither Tello nor McKnight et al., nor any other cited reference shows that the sender of the message is authenticated using a public/private key and that the recipient is also verified using a globally unique identifier (GUID). Thus, Claims 1-4, 8-14, 17-20, 24, 27-28 and 32 and their progeny are believed allowable.

Claims 6, 16, 22, 26 and 30 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Tello in view of McKnight et al., and further in view of U.S. Pat. No.6,704,789 to Ala-Laurila et al. (hereinafter, "Ala-Laurila et al."). This rejection is respectfully traversed and Claims 6, 16, 22, 26 and 30 are believed allowable based on the foregoing and following discussion.

Claims 6, 16 and 22 are believed allowable as being based on allowable base claims, as discussed above. Applicant further maintains that the combination of Tello with Ala-Laurila et al. is improper because Tello teaches away from implementation of network transmission. Tello

teaches that the smartcard is directly connected to the processor to determine authorization. This teaches away from communicating with the processor over a network transmission, as taught by Ala-Laurila et al. Further, Ala-Laurila et al. teach a system to authenticate a user on a network. Tello teaches a method for authenticating a smartcard (held by a user) on a system. Neither cited references teach authenticating an authorized party sending a message to enable optional features of a system resource, while also verifying the intended recipient using a globally unique identifier (GUID), as discussed above. Thus, not only do Tello and Ala-Laurila et al. not show all of the features of the recited claims, either separately, or in combination with each other or combination with McKnight et al., there is no motivation to combine the cited references. Further, the Examiner asserts that the motivation is that network transmission is an effective method of communication, even while Tello teaches away from this by forcing the smartcard to be directly connected to the system. Moreover, combining the references will not result in Applicant's claimed invention. Thus, Claims 6, 16, 22, 26 and 30 are believed allowable and should be permitted to issue at the earliest possible time.

Claims 7, 15 and 23 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Tello in view of McKnight et al., and further in view of U.S. Pub. No. 2001/0025312 to Obata (hereinafter, "Obata"). This rejection is respectfully traversed and Claims7, 15 and 23 are believed allowable based on the foregoing and following discussion.

Claims 7, 15 and 23 are believed allowable as being dependent on allowable base claims, as discussed above.

Claim 29 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Tello in view of U.S. Pat. No. 6,393,559 to Alexander (hereinafter, "Alexander"). This rejection is respectfully traversed and Claim 29 is believed allowable at least by being based on an allowable base claim, as discussed above. The Examiner has failed to make a *prima facie* case of anticipation for base Claim 27. The Examiner has not shown that each and every element of the base claim is taught by Tello. For instance, Claim 27 (and 29) require an authenticator to decrypt, authenticate (public/private key) and verify the secure message (using a GUID) and to *discard the secure message if failure occurs during any one of decryption, authentication and verification.*

Therefore, Claim 27 and its progeny, including Claim 29 are believed allowable. Further, Alexander teaches a system which may reboot a platform upon a failure to boot the first time, in order to correct the problem. It will be apparent to one of ordinary skill in the art that fixing a hardware problem is not the same as enabling the BIOS to control the at least one of the *optional* features of a system resource. Alexander does not teach optional features, but teaches rebooting to correct a hardware error, for instance, to reinitialize corrupted memory and change a flag from "resume from suspend" to "full reboot." (See Col. 3, lines 16-22) Moreover, Alexander does not teach or suggest a reboot according to a received secure message. Therefore, combining Tello and Alexander will not result in Applicant's claimed invention.

Moreover, there is no motivation to combine the references. The Examiner asserts that "it would have been obvious...to combine...and incorporate the functionality of rebooting to ensure proper initialization and rectify possible glitches." However, as discussed above, the Examiner once again begs the question. Further, Tello teaches away from a reboot in that a smartcard is used to authenticate the user at boot time. There is no suggestion that if the smartcard fails to authenticate the user that the system should be rebooted because that would be counterintuitive. The purpose of authenticating the user is to prevent a boot unless the user is authorized. Further, Tello teaches that once authorized, the system is booted according to the user's access level and there would be no point in rebooting after the boot. It would serve no purpose. Thus, the Examiner has failed to provide a *prima facie* case of obviousness, and has also failed to provide actual evidence of a suggestion to modify a prior art reference or to combine multiple prior art references. Therefore, Claim 29 is believed allowable and should be permitted to issue at the earliest possible time.

Claim 31 is rejected under 35 U.S.C. § 103 (a) as being unpatentable over Tello in view of McKnight et al. and further in view of U.S. Pat. Application No. 2003/0052906, now U.S. Pat. No. 6,633,309, to Lau et al. (hereinafter, "Lau et al."). This rejection is respectfully traversed and Claim 31 is believed allowable base on the foregoing and following discussion.

The Examiner asserts that Lau et al. teach *the secure message comprises executable code to be used as a Dynamically Loaded Library (DLL), and wherein the DLL is to be stored in non-volatile storage coupled to the BIOS, and wherein the DLL is to be loaded by the BIOS at run-*

time. This assertion is flawed. Lau et al. teach putting plug-in modules in dynamic link libraries (DLL). Lau et al. do not teach or suggest that the DLLs are to be loaded by the BIOS at run-time. Lau et al. teach that

> "For a Microsoft Windows operating system environment, the plug-ins 16 are compiled as dynamic link libraries. At processing environment 10 run time, the shell 14 scans a predefined directory for plug-in programs. When present, a plug-in program name is added to a list which is displayed in a window or menu for user selection. When an operator selects to run a plug-in 16, the corresponding dynamic link library is loaded into memory and a processor begins executing instructions from one of a set of pre-defined entry points for the plug-in. To access a video sequence and video object segmentations, a plug-in uses a set of callback functions. A plug-in interfaces to the shell program 14 through a corresponding application program interface module 18." (Para. 37)

The Windows® run-time environment is discussed, but at no time do Lau et al. ever teach or suggest that the plug ins are coupled to or loaded by the BIOS. Further, Claim 31 is believed allowable as being dependent on an allowable base claim, as discussed above. Therefore, the Examiner has failed to show a *prima facie* cases of obviousness and Claim 31 should be allowed to issue at the earliest possible time.

Claims 5, 21 and 25 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Tello in view of McKnight et al. and further in view of U.S. Patent No. 6,584,561 to Merkin et al. (hereinafter "Merkin et al."). This rejection is respectfully traversed and Claims 5, 21 and 25 are believed allowable based on the foregoing and following discussion.

Merkin et al. disclose a system and method for restricting a compact disk (CD) containing boot software to work only on computer systems for which the boot software has been authorized to operate. Merkin et al. do not teach or suggest *splicing the contents of a message into the BIOS execution path*, as recited in the claims. Merkin et al. disclose that a computer system is checked for predetermined identification criteria to allow boot software from a CD to run on the computer system. Merkin et al. teach that a computer system may boot using the boot software on the CD. At no time do Merkin et al. disclose that a message is sent or that the contents of the message are used to alter a portion of the existing BIOS during boot. Instead, Merkin et al. teach a system where the system is booted using the entire boot software on the CD, not contents of a message. Merkin et al. teach replacing the existing boot software (BIOS) with the software on the CD to

provide new boot software (Col. 2, lines 34-38). Applicant further points out that the limitations of Claims 5 and 25 are similar to claim 21. In the Office Action dated Aug. 5, 2006, the Examiner states that

> "Applicant's arguments with respect to the rejection(s) of claim(s) 21 have been fully considered and are persuasive. Neither Tello nor Merkin disclose the limitations of claim 21 as correctly noted by the applicant."

As such, the Examiner conceded that Merkin et al. did not show the limitations of Claim 21. Therefore, this rejection is improper and must be withdrawn. The addition of citing McKnight et al. as combined with Tello and Merkin et al. is improper and will not result in Applicant's invention. Also, the limitation asserted to be shown by Merkin et al. that was overcome in the previous response (i.e. splicing), is not shown by McKnight et al., sp this combination is gratuitous. Moreover, Applicant pointed out this erroneous rejection in the Response dated 20 March 2006. However, the subsequent office actions failed to provide any contrary evidence that Merkin et al. teaches the claimed limitation, or address Applicant's response at all. Similarly, the Examiner fails to make a *prima facie* case of obviousness for Claims 5 and 25, as well as Claim 21. In addition to the arguments present above, the cited prior art does not teach or suggest splicing content of the message into an execution path of the BIOS. **Thus, because the Examiner relies on an argument that Applicant has previously overcome, Applicant respectfully requests that the Examiner reissue a new non-final office action without citing the improper reference.**

In addition, none of the cited prior art, either alone or in combination, teaches that the message has been sent by the authorized party using a digital signature in the message and a public key stored in a non-volatile storage communicatively coupled to the BIOS and the verification that the system is an intended recipient of the message, wherein verifying comprises comparing an identifier in the message against a globally unique identifier (GUID) of the system. All claims remaining in the application are now allowable.

CONCLUSION

In view of the foregoing, Claims 1, 3-11, 13-17 and 19-32 are all in condition for allowance. If the Examiner has any questions, the Examiner is invited to contact the undersigned at (703) 633-6845. Early issuance of Notice of Allowance is respectfully requested. Please charge any shortage of fees in connection with the filing of this paper, including extension of time fees, to Deposit Account 02-2666 and please credit any excess fees to such account.

Respectfully submitted,

Dated: 17 Oct. 2006

/Joni D. Stutman-Horn/

Joni D. Stutman-Horn, Reg. No. 42,173
Patent Attorney
Intel Corporation
(703) 633-6845

c/o Blakely, Sokoloff, Taylor &
Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026